государственное бюджетное общеобразовательное учреждение Самарской области
средняя общеобразовательная школа пос. Новый Кутулук
муниципального района Борский Самарской области

C=RU, O=ГБОУ СОШ пос. Новый Кутулук, CN=Колосова Н_М_, E=nkutuluk_sch@samara.edu.ru
00c3a0b80fde361dae
2023-05-05 10:00:33

УТВЕРЖДАЮ
Директор ГБОУ СОШ
пос. Новый Кутулук
_____/Н.М.Колосова/
от 31.08.2021г.

Рабочая программа
по внеурочной деятельности
« Информационная безопасность»
для обучающихся 8 класса

Возраст обучающихся: 14-15 лет
Срок реализации: 1 год

Составитель (разработчик):
Незнамова Н.И.

РАССМОТРЕНО
На заседании методического объединения
естественно-математического цикла
Протокол № 1 от 31.08.2021г.
Руководитель м/о _____/Н.С. Хамина/

ПРИНЯТО
на заседании педагогического совета
Протокол № 1 от 31.08.2021г.
Председатель п/с _____/Н.М. Колосова/

Пояснительная записка

Рабочая программа внеурочной деятельности «Информационная безопасность» по общеинтеллектуальному направлению составлена на основе Федерального государственного образовательного стандарта основного общего образования, Основной образовательной программы основного общего образования ГБОУ СОШ пос. Новый Кутулук на 2021-2022 учебный год, Примерной программы внеурочной деятельности.

Курс внеурочной деятельности «Информационная безопасность» рассчитан на общее число учебных часов за год обучения 34 (1 час в неделю).

Данная программа предназначена для учащихся 8 класса.

Планируемые результаты

Предметные:

Обучающийся научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,
- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Обучающийся овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Обучающийся получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления

осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет- ресурсы и другие базы данных.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновениюсвязи между явлениями, из этих обстоятельств выделять определяющие, способные быть причиной данного явления, выявлять причины и следствия явлений;
- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;

- использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Личностные.

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационнойсреде.

Содержание курса

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

- Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Тема 2. С кем безопасно общаться в интернете. 1 час.

- Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.

- Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.

Тема 4. Безопасный вход в аккаунты. 1 час.

- Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.

- Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.

Тема 6. Публикация информации в социальных сетях. 1 час.

- Персональные данные. Публикация личной информации.

Тема 7. Кибербуллинг. 1 час.

- Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.

Тема 8. Публичные аккаунты. 1 час.

- Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.

Тема 9. Фишинг. 2 часа.

- Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

- **Выполнение и защита индивидуальных и групповых проектов. 3 часа.**

Раздел 2. «Безопасность устройств»

Тема 1. Что такое вредоносный код. 1 час.

- Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.

Тема 2. Распространение вредоносного кода. 1 час.

- Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема 3. Методы защиты от вредоносных программ. 2 час.

- Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.

Тема 4. Распространение вредоносного кода для мобильных устройств. 1 час.

- Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.

Раздел 3 «Безопасность информации»

Тема 1. Социальная инженерия: распознать и избежать. 1 час.

- Приемы социальной инженерии. Правила безопасности при виртуальных контактах.

Тема 2. Ложная информация в Интернете. 1 час.

- Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.

Тема 3. Безопасность при использовании платежных карт в Интернете. 1 час.

- Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.

Тема 4. Беспроводная технология связи. 1 час.

Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.

Тема 5. Резервное копирование данных. 1 час.

Безопасность личной информации. Создание резервных копий на различных устройствах.

Тема 6. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.

Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.

Выполнение и защита индивидуальных и групповых проектов. 3 часа.

Повторение. Волонтерская практика. 3 часа.

Программа предусматривает следующие виды деятельности:

- Игровая деятельность
- Познавательная деятельность

- Проблемно – ценностное общение

Формы проведения занятий: доклады, презентации, проекты, памятки, онлайн занятия.

Тематическое планирование

№ п/п	Тема урока	Количество часов
Тема 1. «Безопасность общения»		
1	Общение в социальных сетях и мессенджерах	1
2	С кем безопасно общаться в интернете	1
3	Пароли для аккаунтов социальных сетей	1
4	Безопасный вход в аккаунты	1
5	Настройки конфиденциальности в социальных сетях	1
6	Публикация информации в социальных сетях	1
7	Кибербуллинг	1
8	Публичные аккаунты	1
9	Фишинг	2
10	Выполнение и защита индивидуальных и групповых проектов	3
Тема 2. «Безопасность устройств»		
1	Что такое вредоносный код	1
2	Распространение вредоносного кода	1
3	Методы защиты от вредоносных программ	2
4	Распространение вредоносного кода для мобильных устройств	1
5	Выполнение и защита индивидуальных и групповых проектов	3
Тема 3 «Безопасность информации»		

1	Социальная инженерия: распознать и избежать	1
2	Ложная информация в Интернете	1
3	Безопасность при использовании платежных карт в Интернете	1
4	Беспроводная технология связи	1
5	Резервное копирование данных	1
6	Основы государственной политики в области формирования культуры информационной безопасности	2
7	Выполнение и защита индивидуальных и групповых проектов	3
8	Повторение, волонтерская практика, резерв	3